UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/920,554	08/01/2001	Graeme John Proudler	B-4240 618934-9	4232

22879 7590 04/17/2008

HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER	
DAVIS, ZACHARY A	
ART UNIT	PAPER NUMBER
2137	

NOTIFICATION DATE	DELIVERY MODE
04/17/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM
mkraft@hp.com
ipa.mail@hp.com

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/920,554
Filing Date: August 01, 2001
Appellant(s): PROUDLER, GRAEME JOHN

Robert Popa
(Reg. No.)
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 04 January 2008 appealing from the Office action mailed 27 June 2006.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6,289,462	MCNABB et al	09-2001
6,327,652	ENGLAND et al	12-2001

"HP Virtualvault Trusted Web-Server Platform Product Brief". Hewlett-Packard Company, Jan. 1999, pp. 1-6

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

Claims 1-6, 14-26, 29, and 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over McNabb, US Patent 6289462, in view of England et al, US Patent 6327652.

In reference to Claims 1 and 2, McNabb discloses a method including a requester providing a specification of a service to be performed that establishes required sensitivity levels for processes in the service (see, for example, column 19, line 55-column 20, line 2, where different processes are specified for different sensitivity levels) and a computing platform executing the service according to the specification (see the Trusted Server of Figure 1, and column 5, lines 20-29) and logging performance of the processes and providing the log to the requestor (the audit trail described at column 7, lines 28-33). However, although McNabb discloses sensitivity levels that describe required security (column 8, lines 33-37 and 10-15) and that there is a trusted computer system (column 8, lines 40-45), McNabb does not explicitly disclose details of establishing the trust in the computer system, nor does McNabb explicitly disclose levels of trust.

England discloses a method in which an operating system is securely loaded where each component of the system is associated with a trust level (column 4, lines 5-11) and each application is also determined to be trusted or non-trusted (column 9, lines 11-20). England also discloses a requester providing a specification of a service to be performed that establishes required trust levels for processes in the service (column 9, lines 42-51; column 19, lines 13-40). England further discloses logging performance (see, for example, column 4, lines 18-23). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of McNabb to incorporate levels of trust as taught by England, in order to guarantee the ability to distinguish between trusted and non-trusted systems executing on the same computer (see England, column 3, lines 56-61).

In reference to Claim 3, McNabb further discloses a protected computing environment (see Figure 1).

In reference to Claims 4 and 23, McNabb further discloses measuring integrity of the platform (see column 8, lines 40-45, regarding the trusted computer system). England also discloses monitoring integrity (see, for example, column 12, lines 53-65).

In reference to Claim 5, McNabb further discloses a management process that allocates the execution of processes and logging to environments associated with the platform (see column 21, lines 34-55).

In reference to Claim 6, McNabb further discloses the management process within the protected environment (see column 21, line 34-column 22, line 2).

In reference to Claim 14, McNabb further discloses that a process may be swapped between environments (see column 11, line 66-column 12, line 14).

In reference to Claims 15-20, McNabb further discloses logging input data, output data, and executed program instructions of a process (see column 7, lines 28-33; column 23, lines 26-35).

In reference to Claim 21, McNabb further discloses encrypting the logging data (column 23, lines 26-35, where the audit record is protected).

In reference to Claim 22, McNabb further discloses the specification of the service establishing logging parameters for the processes (column 23, lines 26-35).

In reference to Claim 24, McNabb discloses a platform including a protected computing environment (see Figure 1) and one or more compartments (column 17, lines 9-14), in which processes may be executed for a user in the compartments and the results of the processes may be returned to the user as trustworthy data from the protected environment (see, for example, column 6, lines 20-23), and where the platform further includes a management process that receives a service description including required

sensitivity levels for processes within the service (see, for example, column 19, line 55-column 20, line 2, where different processes are specified for different sensitivity levels) and that allocates the processes to the compartments (column 21, lines 34-55). However, although McNabb discloses sensitivity levels that describe required security (column 8, lines 33-37 and 10-15) and that there is a trusted computer system (column 8, lines 40-45), McNabb does not explicitly disclose details of establishing the trust in the computer system, nor does McNabb explicitly disclose levels of trust.

England discloses a system in which an operating system is securely loaded where each component of the system is associated with a trust level (column 4, lines 5-11) and each application is also determined to be trusted or non-trusted (column 9, lines 11-20). England further discloses receiving a service description including required trust levels for processes in the service (column 9, lines 42-51; column 19, lines 13-40). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the platform of McNabb to incorporate levels of trust as taught by England, in order to guarantee the ability to distinguish between trusted and non-trusted systems executing on the same computer (see England, column 3, lines 56-61).

In reference to Claim 25, McNabb further discloses that the compartments may be located outside the protected environment (Figure 12; column 17, lines 57-61).

In reference to Claim 26, McNabb further discloses that the compartments may be located inside the protected environment (Figure 12; column 17, lines 57-61).

In reference to Claim 29, McNabb further discloses measuring integrity of the platform (see column 8, lines 40-45, regarding the trusted computer system). England also discloses monitoring integrity (see, for example, column 12, lines 53-65).

In reference to Claim 31, McNabb further discloses the management process within the protected environment (column 21, line 34-column 22, line 2).

Claims 7-13, 27, and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over McNabb in view of England as applied to claims 5 and 24 above, and further in view of "HP Virtualvault Trusted Web-Server Platform Product Brief", hereinafter "Virtualvault".

In reference to Claim 7, McNabb as modified by England discloses everything as applied to Claim 5 above. McNabb further discloses the use of compartments (see, for example, column 17, lines 9-14). However, McNabb does not explicitly disclose that the compartment contains a protected computing engine, nor does England. Virtualvault discloses a computing platform that includes the use of compartments, which include protected computing engines (see page 3, "Data Partitioning Separates and Secures Files"). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of McNabb and England to include compartments containing protected computing engines, in order to provide security for web servers (see Virtualvault, page 2, "Virtualvault: The Answer to Secure Access").

In reference to Claim 8, Virtualvault further discloses a Java virtual machine (see page 4, "A 'Vaulted' Java Virtual Machine").

In reference to Claim 9, McNabb further discloses that one or more compartments are located in the protected environment (see Figure 12; column 17, lines 57-61). Further, Virtualvault further discloses that one or more compartments are located within the protected environment (see page 3, the INSIDE compartment).

In reference to Claim 10, McNabb further discloses that the computing engine is prohibited from operating on input data if it is not permitted to do so (see column 8, lines 10-15 on Mandatory Access Control).

In reference to Claim 11, McNabb further discloses that input data and processes are each provided with a type, and that the operation is prevented if the types do not match (see column 8, lines 10-15 on Mandatory Access Control).

In reference to Claims 12 and 13, McNabb further discloses that the input data may have an owner, and that the process may be required to inform the owner of the use of the data or to obtain consent from the owner to use the data (see column 8, line 54-column 9, line 4).

In reference to Claims 27 and 28, McNabb as modified by England discloses everything as applied to Claim 24 above. However, McNabb does not explicitly disclose that the compartment contains a protected computing engine, specifically a Java virtual machine, nor does England. Virtualvault discloses a computing platform that includes the use of compartments, which include protected computing engines (see page 3, "Data Partitioning Separates and Secures Files"). Virtualvault further specifically discloses a Java virtual machine (see page 4, "A 'Vaulted' Java Virtual Machine"). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the system of McNabb and England to include compartments containing protected computing engines, specifically Java virtual machines, in order to provide security for web servers (see Virtualvault, page 2, "Virtualvault: The Answer to Secure Access").

(10) Response to Argument

Issue 1: Whether claims 1-6, 14-26, 29, and 31 are patentable under 35 U.S.C. 103(a) over McNabb in view of England.

In reference to the rejection of independent Claim 1, Appellant first substantially repeats the arguments set forth in the reply received 07 April 2006 (see pages 8-13 of the present Appeal Brief). As summarized in the present Appeal Brief (pages 13-14), these arguments were previously addressed in the final Office action mailed 27 June 2006. The Examiner's responses and clarifications thereto are provided below for convenience.

In reference to Claim 1, Appellant argues that there is no motivation to combine the references, that there is "no reasonable expectation that a person of ordinary skill could combine the references in any meaningful way", and that the suggested combination does not anticipate the claims (see page 11 of the present Appeal Brief).

In response to Appellant's argument that there is no suggestion to combine the references, the Examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, the motivation is to be found in England, as cited in the previous Office action, namely to guarantee the ability to distinguish between trusted and non-trusted systems executing on the same computer (see England, column 3, lines 56-61).

In response to the statement that there is "no reasonable expectation that a person of ordinary skill could combine the references in any meaningful way", the Examiner notes that this is not actually the test

set forth in the MPEP as quoted on pages 10-11 of the present Appeal Brief. Rather, the criterion is whether there is a "reasonable expectation of success". The Examiner believes that because both the McNabb and England references are directed to secure and/or trusted operating systems, and are therefore analogous art, there would be a reasonable expectation that one would be successful in combining features from the two systems.

In response to Appellant's argument that neither England, McNabb, nor "any reasonable combination of the two" suggests the claimed limitation of "a requestor providing a specification of a service to be performed to the computing platform, wherein the specification of service establishes specified levels of trust for at least one of the processes in the service" (pages 11-12 of the present Appeal Brief), the Examiner respectfully disagrees. The Examiner notes that both McNabb and England at least suggest a requestor providing a specification of a service to be performed (see McNabb, as cited, column 19, line 55-column 20, line 2; see also, for example, England, column 9, lines 42-51, noting that a requestor provides a specification of a service, namely the downloading of specific content) and that England, at least, suggests that levels of trust are specified for at least one process (see England, column 19, lines 13-40, where trust levels specifying required functions to access certain content or processes are specified in an access control list).

The Examiner notes that other assertions and statements made by Appellant do not appear to be supported by specific citations from the references or elsewhere (see, for example, the second and third paragraphs on page 10 of the present Appeal Brief, noting the Appellant states that England "seems to say", or in the first paragraph on page 13 of the present Appeal Brief, where Appellant states that England "seems to suggest"). Therefore, without any explicit support for such interpretations and statements, those assertions and statements are not persuasive as evidence.

To further clarify the above responses, in response to the argument that neither England, McNabb, nor their combination suggests "a requestor providing a specification of a service to be performed to the computing platform, wherein the specification of service establishes specified levels of trust for at least one of the processes in the service" (pages 11-12 of the present Appeal Brief), the Examiner notes that both McNabb and England at least suggest a requestor providing a specification of a service to be performed. The above cited portion of McNabb clearly discloses a requestor providing a specification of a service to be performed, and discloses that levels of sensitivity of access are specified for the processes of the service (see column 19, line 55-column 20, line 38, where access is controlled to processes in software by defining privileges or sensitivity levels required to perform the process). The above cited portions of England also generally discloses providing a specification of a service to be performed (see column 9, lines 42-51, where a service can be, for example, downloading specific content) and explicitly discloses that levels of trust are specified for at least one process (column 19, lines 13-40, where, as described above, trust levels specifying required functions to access certain content or processes are specified in an access control list). Therefore, although the services requested may not be identical, both McNabb and England disclose a requester providing a specification of a service to be performed within the scope of the present claim. Further, the combination would have fairly suggested to one of ordinary skill in the art the incorporation of the levels of trust in England in addition to the measures disclosed by McNabb (namely sensitivity levels describing required security, and trusted computer systems in general), for the reasons detailed above.

In new arguments, Appellant "notes that client and server are well known in the art as being distinct entities" (page 15 of the present Appeal Brief), which the Examiner does not dispute; however, Appellant also "submits that it seems a bit fast to conclude that McNabb and England are analogous art" and further "submits that the Examiner has failed to show why or how a combination of McNabb and England would

'guarantee' the ability to distinguish between trusted and non trusted systems executing on the same computer" (pages 15-16 of the present response, where the latter is directed to the motivation to combine the references as cited above, and found at England, column 3, lines 56-61). The Examiner respectfully disagrees with the latter two assertions, noting that Appellant does not provide any specific evidence in support of these allegations. Additionally, the portions of McNabb and England cited later in the present brief in support of the assertion that the combination would not have led the skilled person to a method as claimed do not provide sufficient support for the assertions noted above. In particular, although Appellant states that "England discloses (column 3, lines 56-61) distinguishing between a digital rights management operating system from a non-trusted operating system on the same computer, wherein the computer is a client computer (column 8, lines 42-43)" (page 17 of the present Appeal Brief, emphasis Appellant's), the Examiner notes that the first cited portion of England (in column 3) does not explicitly mention the type of computer on which the operating system(s) would be running, and the second cited portion of England (in column 8) only describes a client computer as a non-limiting example of a computer on which such an operating system would be running. Further, Appellant states that "McNabb discloses a 'trusted' operating system on a 'trusted' server computer (column 8, lines 54-58)" (page 17 of the present Appeal Brief, emphasis Appellant's). However, the Examiner notes that while this is an example embodiment of a trusted computer as described in McNabb, the disclosure in McNabb is more general in that McNabb disclosure can relate to computer systems in general (see column 1, lines 12-17, generally describing the field of the McNabb reference, and more particularly, column 8, lines 40-45, describing a general trusted computer system, which is not necessarily a server).

In response to Appellant's argument that the combination of McNabb and England would at most result in "a system having: a client computer as disclosed in England communicating with a content

provider trusted server with a trusted operating system as disclosed in McNabb" and various aspects of such a hypothetical combination (see pages 17-18 of the present Appeal Brief), the test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference; nor is it that the claimed invention must be expressly suggested in any one or all of the references. Rather, the test is what the combined teachings of the references would have suggested to those of ordinary skill in the art. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981). Further, Appellant admits such a combination is hypothetical speculation, and does not provide any specific citations of evidence from the references to support the combination described therein. Additionally, as described above, the Examiner again notes that the limited portions of England and McNabb that are cited do not clearly limit the disclosure of England to clients and McNabb to servers, but instead both references are more generally directed to aspects of secure operating systems (although specific embodiments within the references may be explained with respect to one or another of client or server systems). Additionally, as described above, the Examiner notes that, one of ordinary skill in the art would have found it obvious to modify the method of McNabb by incorporating the teachings of England, in order to yield the claimed method, for the reasons detailed above.

In response to Appellant's argument that the references fail to show certain features of Appellant's invention, it is noted that the features upon which Appellant relies (i.e., "creating a log of the performance of specific processes only", see page 20 of the present Appeal Brief, emphasis added) are not recited in the rejected claims. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). Specifically, Appellant argues that both McNabb and England teach recording or logging indistinctly any operation or process performed in the systems and that this teaches away from the claimed

limitation of "a log of the performance of the processes performed according to the specified levels of trust" (pages 19-21 of the present Appeal Brief). The Examiner fails to appreciate this argument. If every process or operation in the system is logged, then clearly any processes performed according to specified levels of trust are logged, as claimed. These specific processes are encompassed by the processes that are logged, since all processes are logged. Although Appellant asserts that McNabb and England "fail to disclose or suggest creating a log of the performance of specific processes only" (pages 20-21 of the present Appeal Brief, emphasis added), this is not what is claimed. The claim does not exclude the logging of processes that may not have been performed according to the specific levels of trust; rather, the claim recites a log of the performance of the processes performed according to the specified levels of trust without further limiting what else may or may not be included in such a log.

Further, Appellant notes that "according to the analysis of the Examiner, the requestor of McNabb is a user requesting an object in the system and the requestor of England is a user requiring the downloading of specific content" (pages 21 of the present Appeal Brief). However, because Appellant does not further elaborate on this point, the Examiner fails to appreciate this argument. Additionally, to reiterate the point above, the Examiner notes that although the services requested may not be identical, both McNabb and England disclose a requester providing a specification of a service to be performed, within the scope of the present claim (see McNabb, column 19, line 55-column 20, line 38; see also England, column 9, lines 42-51).

Finally, Appellant notes that the audit track of McNabb (corresponding to the claimed log) "is in an isolated partition protected by ... access control mechanisms to prevent intruders from cover their tracks and eliminating traces of penetration attempts to maintain sufficient evidence" (see pages 21-22 of the present Appeal Brief; although there is no citation, this appears to refer to the disclosure of McNabb at

column 23, lines 26-35), asserting that this teaches away from providing a requester with a log. However, the Examiner notes that access control mechanisms that prevent covering of tracks or elimination of evidence do not necessarily constitute a teaching away from providing a user with a log. In particular, although these access controls clearly prevent writing to the audit tracks or logs as noted in the above portion of McNabb, there is nothing to suggest that read access to the audit trails is limited in any way, which would be the requirement to forestall the provision of such a log to a user. See also column 7, lines 28-33, discussing the tracing of events using the audit trails. Appellant also asserts that "the boot log of England is not provided to the user" (page 22 of the present Appeal Brief); however, Appellant provides no evidence in support of such an allegation. While the boot log of England is also protected from tampering (see, for example, column 4, lines 18-23), this does not constitute a teaching away from providing such a log to the requester.

In reference to independent Claim 24, Appellant first substantially repeats the arguments set forth in the reply received 07 April 2006 (see pages 22-23 of the present Appeal Brief). As summarized in the present Appeal Brief (page 24), these arguments were previously addressed in the final Office action mailed 27 June 2006.

Further in reference to independent Claim 24, Appellant substantially repeats and/or refers back to the arguments presented in reference to independent Claim 1 (see pages 24-27 of the present Appeal Brief); such arguments were addressed above.

Further, in reference to dependent Claims 2-6, 14-23, 25, 26, 29, and 31, Appellant does not argue the merits of the claims separately and only relies on their dependence on Claims 1 and 24 (see page 27 of the present Appeal Brief).

Issue 2: Whether claims 7-13, 27, and 28 are patentable under 35 U.S.C. 103(a) over McNabb in view of England and further in view of Virtualvault.

In reference to dependent Claims 7-13, 27, and 28, Appellant asserts that the Virtualvault reference has further not been shown to disclose or suggest limitations of independent Claims 1 and 24 (page 28 of the present Appeal Brief); however, as noted above, the noted limitations have been shown to be disclosed by the combination of McNabb and England. Appellant does not provide any further arguments as to the separate patentability of dependent Claims 7-13, 27, and 28 apart from the arguments presented with respect to the independent Claims, as addressed above. The Examiner notes that Appellant asserts that "claims 1 and 24 are patentable over McNabb in view of Virtualvault" and also that "claims 7-13 and claims 27-28 are patentable over McNabb in view of Virtualvault" (page 28 of the present Appeal Brief); however, the Examiner notes that these combinations were not the grounds of rejection relied upon. Rather, Claims 1 and 24, as set forth above, were rejected as unpatentable over McNabb in view of England, and Claims 7-13, 27, and 28, were rejected as unpatentable over McNabb in view of England and further in view of Virtualvault.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Zachary A. Davis

/Zachary A Davis/
Examiner, Art Unit 2137

Conferees:

/KIMYEN VU/

Supervisory Patent Examiner, Art Unit 2135

/HOSUK SONG/

Primary Examiner, Art Unit 2135